

SECRET

What is Claimed is:

1. A method comprising:
selectively hashing a first data string;
digitally signing a second data string; and
generating an encryption key based on the digitally signed second data string and a third data string.
2. The method as recited in Claim 1, further comprising:
selectively encrypting data using the encryption key.
3. The method as recited in Claim 2, wherein the data includes the hash of the first data string.
4. The method as recited in Claim 2, wherein the data includes the first data string.
5. The method as recited in Claim 4, further comprising:
storing the encrypted data, the second data string and the third data string.
6. The method as recited in Claim 5, wherein the encrypted data, the second data string and the third data string are each stored in memory.
7. The method as recited in Claim 5, wherein the encrypted data, the second data string and the third data string are each stored on a storage medium.

32. The arrangement as recited in Claim 31, wherein the first logic is further configured to selectively encrypt data using the encryption key.

33. The arrangement as recited in Claim 32, wherein the data includes the hash of the first data string.

34. The arrangement as recited in Claim 32, wherein the data includes the first data string.

35. The arrangement as recited in Claim 34, wherein the first logic is further configured to store the encrypted data, the second data string and the third data string.

36. The arrangement as recited in Claim 35, further including memory operatively coupled to the first logic, and wherein the first logic stores the encrypted data, the second data string and the third data string are in the memory.

37. The arrangement as recited in Claim 35, further including a data storage device having at least one storage medium, the data storage device being operatively coupled to the first logic, and wherein the first logic provides the encrypted data, the second data string and the third data string to the storage device for storage on a storage medium.

51. The method as recited in Claim 50, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

52. The method as recited in Claim 50, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

53. The method as recited in Claim 44, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a substantially randomly generated data string.

54. The method as recited in Claim 44, wherein the first data string, the third data string, and the encrypted data are each accessed by a first device that is configured to selectively hash the first data string and generate the encryption key.

55. The method as recited in Claim 44, wherein a second device digitally signs the second data string.

56. The method as recited in Claim 55, wherein the second device includes a signature-generating device.

57. The method as recited in Claim 56, wherein the signature-generating device is a smart card.

63. The computer-readable medium as recited in Claim 59, wherein accessing the plurality of stored data strings and accessing the encrypted data further includes reading data from at least one storage medium.

64. The computer-readable medium as recited in Claim 58, wherein generating at least a portion of the encryption key further includes cryptographically hashing at least a portion of the digitally signed second data string combined with at least a portion of the third data string.

65. The computer-readable medium as recited in Claim 64, wherein generating the encryption key further includes cryptographically hashing the digitally signed second data string concatenated with the third data string.

66. The computer-readable medium as recited in Claim 64, wherein generating the encryption key further includes cryptographically hashing the third data string concatenated with the digitally signed second data string.

67. The computer-readable medium as recited in Claim 58, wherein at least one data string selected from among the first data string, the second data string and the third data string includes a substantially randomly generated data string.

